PROCEDURE FOR HANDLING REQUESTS TO EXERCISE RIGHTS BY DATA SUBJECTS

In accordance with EU Regulation 679/2016 and Legislative Decree 196/2003 and subsequent amendments

SUMMARY

INTRODUCTION

APPLICATION PURPOSE

The purpose of this procedure is to define the activities, roles, and responsibilities that the Data Controller undertakes in handling requests received from data subjects to exercise their rights within the scope of personal data protection.

This procedure is made known to all individuals authorized to process personal data, including through awareness-raising or training activities.

REGULATORY REFERENCES

ACRONYMS AND DEFINITIONS

GDPR	General Data Protection Regulation (EU) 2016/679

Supervisory Authority	Data Protection Authority responsible for monitoring and enforcing data protection regulations.
DPO or RPD (Data Protection Officer or Responsible for Data Protection)	A professional figure with specific expertise in information technology, legal, risk assessment, and process analysis, whose main task is to observe, evaluate, and direct the methods of personal data processing to ensure compliance with European and national privacy regulations.
Privacy Officer	A person designated by the Data Controller to serve as a contact point for compliance with personal data protection regulations and related obligations.
Data Subject	A natural person whose personal data is processed by the Data Controller or Data Processor.
Data Controller	The natural or legal person, public authority, service, or other body that, alone or jointly with others, determines the purposes and means of the personal data processing; where the purposes and means of such processing are determined by Union or Member State law, the Data Controller or the specific criteria for their nomination may be provided for by Union or Member State law.
Request for Exercise of Rights	The data subject's right to obtain from the Data Controller confirmation of whether or not personal data concerning them is being processed and, if so, to access the processed personal data.

TYPES OF EXERCISABLE RIGHTS

RIGHT TO ACCESS (Art.15 GDPR)

EXAMPLE
This right is exercisable by the data subject who has the opportunity to request information from the data controller regarding their personal data being processed

Pursuant to Article 15 of EU Regulation 679/2016, the data subject has the right to obtain from the Data Controller confirmation of the existence of personal data processing concerning them and, if so, to access the following information:

- The purposes of the processing;
- The categories of personal data involved;
- The recipients or categories of recipients to whom personal data has been or will be disclosed, particularly if they are recipients in third countries or international organizations;
- Where possible, the expected retention period for personal data or, if not possible, the criteria used to determine that period;
- The existence of the data subject's right to request the rectification or erasure of personal data or the restriction of processing concerning them or to object to such processing;
- The right to lodge a complaint with a supervisory authority;
- If the data is not collected from the data subject, all available information about its source;
- The existence of automated decision-making, including profiling, referred to in Article 22(1) and (4), and, at least in those cases, meaningful information about the logic involved, as well as the significance and envisaged consequences of such processing for the data subject.

RIGHT TO RECTIFICATION (Art.16 GDPR)

EXAMPLE
This right is exercisable by the data subject who has the possibility to request the modification of their personal data if they believe it is inaccurate or incomplete.

Pursuant to Article 16 of EU Regulation 679/2016, the data subject has the right to obtain from the Data Controller the rectification of inaccurate personal data concerning them without undue delay. Taking into account the purposes of the processing, the data subject has the right to have incomplete personal data completed by providing a supplementary statement.

Under Article 19 of EU Regulation 679/2016, the Data Controller communicates any rectifications, erasures, or restrictions of processing to each of the recipients to whom the personal data has been disclosed, unless this

proves impossible or involves a disproportionate effort. The Data Controller informs the data subject about these recipients upon request.

RIGHT TO ERASURE (Art.17 GDPR)

EXAMPLE
This right is exercisable by the data subject who has the possibility to request the deletion of their personal data, for instance, when the data processing is no longer necessary.

Pursuant to EU Regulation 679/2016, the data subject has the right to obtain from the Data Controller the erasure of personal data concerning them without undue delay, and the Data Controller must erase personal data without undue delay if one of the following reasons applies:

- The personal data is no longer necessary for the purposes for which it was collected or otherwise processed;
- The data subject withdraws consent on which the processing is based, and there is no other legal ground for the processing;
- The data subject objects to the processing under Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing under Article 21(2);
- The personal data has been unlawfully processed;
- The personal data must be erased for compliance with a legal obligation in Union or Member State law to which the Data Controller is subject;
- The personal data has been collected concerning the offer of information society services referred to in Article 8(1).

Where the Data Controller has made the personal data public and is obliged to erase it, they shall, taking account of available technology and the cost of implementation, take reasonable steps, including technical measures, to inform Data Controllers processing the personal data that the data subject has requested the erasure of any links to, or copy or replication of, that personal data.

These actions do not apply to the extent that processing is necessary:

- For exercising the right of freedom of expression and information;
- For compliance with a legal obligation which requires processing by Union or Member State law to which the Data Controller is subject or for the performance of a task carried out in the public interest or the exercise of official authority vested in the Data Controller;
- For reasons of public interest in the area of public health under Article 9(2)(h) and (i) and Article 9(3);
- For archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes under Article 89(1) insofar as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
- For the establishment, exercise, or defense of legal claims.

RIGHT TO RESTRICTION (Art. 18 GDPR)

EXAMPLE
A right exercisable by the data subject who has the possibility to request that their personal data be marked in order to limit their processing.

Under Article 18 of the EU Regulation 679/2016, the restriction of processing may occur in the following cases:

- The data subject disputes the accuracy of personal data, for the period necessary for the data controller to verify the accuracy of such personal data.
- The processing is unlawful, and the data subject opposes the deletion of personal data and instead requests that their use be restricted.
- Although the data controller no longer needs them for processing purposes, the personal data is necessary for the data subject for the establishment, exercise, or defense of a legal claim.
- The data subject has objected to processing under Article 21, paragraph 1, pending verification of whether the legitimate grounds of the data controller override those of the data subject.

If processing is restricted, personal data are processed, except for preservation, only with the consent of the data subject or for the establishment, exercise, or defense of a legal claim or for the protection of the rights of another natural or legal person or for reasons of significant public interest of the Union or a Member State.

RIGHT TO DATA PORTABILITY (Art. 20 GDPR)

EXAMPLE
A right exercisable by the data subject who has the possibility to request the transfer of their personal data. - For example, a request by the data subject to transfer their data to another data controller.

Under Article 20 of EU Regulation 679/2016, the data subject has the right to receive their personal data, which they have provided to a data controller, in a structured, commonly used, and machine-readable format and has the right to transmit those data to another data controller without hindrance from the data controller to whom the data have been provided, where:

- The processing is based on consent under Article 6, paragraph 1, letter a), or Article 9, paragraph 2, letter a), or on a contract under Article 6, paragraph 1, letter b); and
- The processing is carried out by automated means.

RIGHT TO OBJECT (Art. 21 GDPR)

EXAMPLE
A right exercisable by the data subject who has the possibility to withdraw previously given consent. - For example, a request to cease the processing of personal data based on consent with an entity, which had been previously provided.

.Under Article 21 of EU Regulation 679/2016, the data subject has the right to object at any time, due to grounds relating to their particular situation, to the processing of personal data concerning them, including profiling based on those provisions. The data controller shall no longer process the personal data unless they demonstrate compelling legitimate grounds for the processing that override the interests, rights, and freedoms of the data subject, or for the establishment, exercise, or defense of a legal claim.

If personal data are processed for direct marketing purposes, the data subject has the right to object at any time to the processing of personal data concerning them for such marketing, including profiling to the extent that it is related to such direct marketing.

If the data subject objects to processing for direct marketing purposes, personal data shall no longer be processed for such purposes. The right to object is brought to the data subject's attention explicitly and is presented clearly and separately from any other information. In the context of the use of information, society services, and without prejudice to Directive 2002/58/EC, the data subject may exercise their right to object by automated means using technical specifications.

If personal data are processed for scientific or historical research purposes or statistical purposes under Article 89, paragraph 1, the data subject, on grounds relating to their particular situation, has the right to object to the processing of personal data concerning them, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

RIGHT TO ACCESS TO TRANSPARENCY INFORMATION (Art. 1-bis Legislative Decree 152/1997, introduced by Legislative Decree 104/2022)

The employer or public and private contractor is required to inform the employee about the use of decision-making or automated monitoring systems designed to provide relevant information for hiring or assignment of tasks, management, or termination of the employment relationship, allocation of duties or tasks, as well as information related to surveillance, evaluation, performance, and compliance with contractual obligations of employees, by providing the following information:

- The aspects of the employment relationship affected by the use of decision-making or automated monitoring systems.
- The purposes and objectives of the decision-making or automated monitoring systems.
- The logic and functioning of the decision-making or automated monitoring systems.

- The categories of data and the main parameters used to program or train the systems referred to in paragraph 1, including performance evaluation mechanisms.
- Control measures adopted for automated decisions, any correction processes, and the person responsible for the quality management system.
- The level of accuracy, robustness, and cybersecurity of decision-making or automated monitoring systems and the metrics used to measure these parameters, as well as the potentially discriminatory impacts of these metrics.

The employee, either directly or through company or territorial union representatives, has the right to access the data and request additional information regarding information obligations in the case of the use of decision-making or automated monitoring systems. The employer or contractor is required to provide the requested data and respond in writing within thirty days.

RESPONSE PROCEDURE TO DATA SUBJECT'S REQUEST

PHASE 1. PRESENTATION AND RECEIPT OF THE REQUEST

Each entity that receives a request to exercise one of the rights under Article 15 and following the GDPR, is obliged to immediately notify the competent parties, its responsible person, and, for the notification of the request to the Data Controller, the Privacy Referent. The Data Controller notifies the Data Protection Officer (DPO) if appointed, and, if necessary, requests further information on what has been reported.

A request to exercise the rights may also be received by a third party external to the organization, which processes personal data on behalf of the Controller as a Data Processor under Article 28 of the GDPR, who is required to promptly inform the Controller without undue delay.

PHASE 2. ASSESSMENT OF THE REQUEST FEASIBILITY

The Privacy Officer verifies that:

1. The data subject who submitted the request is identified. If reasonable doubts arise during the assessment of the request about the identity of the natural person making it, the Privacy Officer may request further information for the identification of the data subject, transmitting to the data subject the Request for Exercise of Rights Form (Annex A) and the policy. The Privacy Officer keeps track of such requests for additional information in the register of requests.
2. The request is not manifestly unfounded or excessive. If, during the assessment of the request, it appears that the request is manifestly unfounded or excessive, the Privacy Officer may decide whether to respond to the data subject anyway, possibly applying costs, or not respond, reporting the request and the choice to the register of requests (see the next paragraph "manifestly unfounded or excessive requests").

PHASE 3. RETRIEVAL OF DATA AND EXECUTION OF OPERATIONS REQUESTED BY THE DATA SUBJECT

To process the request, the Privacy Officer verifies whether there is processing of personal data and who the Controller is:

- If personal data processing occurs as the Controller, the Privacy Officer proceeds with the response.
- If processing is carried out on behalf of another entity, the Privacy Officer notifies the receipt of the request to the Controller and offers support as required by the appointment.

Once it is confirmed that processing is carried out as the Controller, the Privacy Officer proceeds within the technical and legal limits to exercise the requested rights, informing any joint controllers and data recipients. To properly process the request, the Privacy Officer may involve the competent organizational structures or other external entities involved in the processing, including querying relevant systems.

In cases where legal or regulatory provisions do not allow compliance with what is contained in the request, the appropriate justifications will be prepared, and a response will be provided to the data subject.

PHASE 4. RESPONSE TO THE DATA SUBJECT

The response to the data subject will be provided by the Privacy Officer, with information regarding the action taken regarding the request for the exercise of the rights recognised to them, without undue delay and, in any case, no later than one month from the receipt of the request. This period may be extended by two months, if necessary, considering the complexity and the number of requests received, while informing the data subject of the need for an extension within one month of the request.

The Controller also responds to the data subject in case of non-compliance with the data subject's request, indicating the reasons for non-compliance and the possibility of complaining with a supervisory authority and of filing a judicial remedy.

The response provided to the data subject must always be concise, transparent, and intelligible, and it should be written in plain and clear language.

The response method must take into account the channel used by the data subject to transmit it to the Controller. In particular, if the data subject has submitted the request electronically, the response should preferably, and where possible be provided in the same electronic format, unless otherwise specified by the data subject.

In the case of a request for the exercise of the right to data portability under Article 20 of the GDPR, the response should be provided by attaching the data in electronic format according to the standard outlined in the "Guidelines on the Right to Data Portability" WP242, issued by the European WP29 Group.

Under Article 12, paragraph 2, of the GDPR, in the case of data processing for a purpose that does not require, or no longer requires, the identification of the data subject, the Controller cannot refuse to fulfill the data subject's request for the exercise of their rights, unless the Controller demonstrates that it is unable to identify the data subject. In this latter case, the rights can only be exercised when the data subject provides additional information that allows their identification.

REQUESTS THAT ARE MANIFESTLY UNFOUNDED OR EXCESSIVE

The management of requests for the exercise of rights recognised by the GDPR is carried out at no cost to the data subject. If the data subject's requests are manifestly unfounded or excessive, especially due to their repetitive nature, the data controller may charge a reasonable fee, taking into account the administrative costs incurred to process the request, or refuse to fulfill the request as provided in Article 12, paragraph 5, of the GDPR. It is the responsibility of the data controller to demonstrate the manifestly unfounded or excessive nature of the request.

DOCUMENTATION ARCHIVING

Documentation related to requests for the exercise of rights by data subjects is kept by the data controller.

NOTIFICATION IN CASE OF RECTIFICATION, ERASURE, OR LIMITATION OF PROCESSING

Under Article 19 of the GDPR, the data controller is responsible for notifying each recipient to whom personal data have been transmitted by the data controller, of any rectifications, erasures, or limitations of processing carried out under Articles 16, 17, paragraph 1, and 18 of the GDPR unless this proves impossible or involves a disproportionate effort. The communication to the above-mentioned recipients is made by the data controller within one month from the time of the rectification and/or erasure of data or limitation of processing, and this is tracked in the Register of Requests. If the data subject requests it, the data controller provides evidence of the recipients to whom the data subject's data has been transmitted.

REGISTER OF REQUESTS FOR THE EXERCISE OF DATA SUBJECTS' RIGHTS

The data controller documents requests for the exercise of data subject rights by maintaining an internal register kept in electronic format. The Register of Requests should contain the following information:

- Progressive number;
- Date of receipt of the request;
- Name of the requester;
- Name of the data subject (if different from the requester);

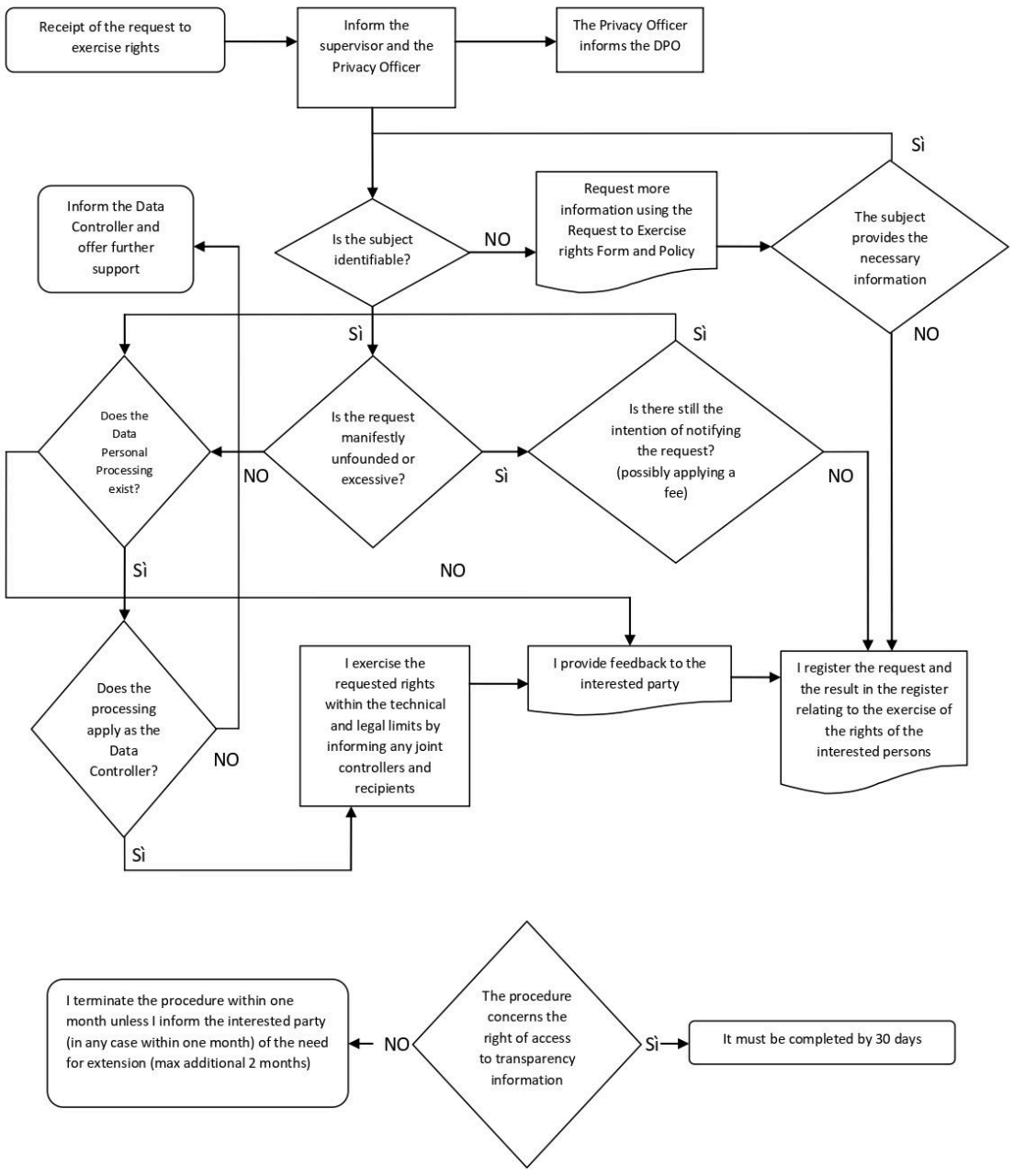
- Description of the request;
- Organisational units or databases involved;
- Action taken regarding the request;
- References of the response note to the data subject (date and any protocol);
- Notes and comments.

INVOLVEMENT OF THE DATA PROTECTION OFFICER

If appointed, the DPO supports the data controller throughout the process of analyzing the likely personal data breach.

SUMMARY OF THE PROCEDURE: FLOWCHART

The management of a request for the exercise of personal rights can be summarized in the phases represented in the following flowchart:



FORMS ATTACHED TO THE PROCEDURE

Annex A - Application form for exercising rights